AFFIDAVIT

I, Chad D. Campanell, being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and have been since December 2000. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I am a graduate of the Criminal Investigator Training Program and the New Professional Training Program at the Federal Law Enforcement Training Center in Brunswick, Georgia. I am currently assigned to a specialized enforcement group, the ATF Arson and Explosives Task Force, whose primary mission is to investigate federal arson and explosive violations. I am an ATF Certified Fire Investigator (CFI) and have specialized training that allows me to opine as to the origin and cause of fires. I am a part time member of ATF's National Response Team (NRT), who responds to large scale fire and explosion scenes for the purpose of determining the origin and cause of those incidents.

2. The information contained in this affidavit is based upon my personal observations and investigation, information relayed to me by other special agents and/or other law enforcement agents, as well as information contained in official reports of law enforcement. Because this affidavit is being submitted for the limited purpose of securing a search warrant for two cellular telephones that were in the possession of NASIR

BILAAL, who was arrested for a violation of Title 18, United States Code, Section 844(i) (maliciously damaging or destroying, or attempting to damage or destroy, by means of fire any building used in interstate commerce), I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause for the search of the cellular telephones possessed by NASIR BILAAL.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

3. The property to be searched are two Apple iPhone cellular telephones recovered from the person of NASIR BILAAL. The cellular telephones are locked, and the serial numbers and other identifying information are unknown. The cellular telephones are physically located at the ATF Group II Office located at 200 Chestnut Street, Room 504, Philadelphia, Pennsylvania, 19106.

4. The first phone is the larger of the two cellular telephones ("Larger Device"). The model number is unknown. The Larger Device is approximately six inches in height and three inches in width. The Larger Device has damage in the form of broken glass on the rear of the phone in the lower left corner as well as damage on the rear of the phone in the upper right corner. The Larger Device has one camera lens on the back side as well as a single flashlight. The rear of the Larger Device is marked with the Apple trademark and the word "iPhone."

5. The second phone is the smaller of the two cellular telephones ("Smaller Device"). The model number is unknown. The Smaller Device is approximately five and a half inches in height and two and five-eighths inches in width. The Smaller Device has no visible physical damage. The Smaller Device has one camera lens on the back side as well as a single flashlight. The rear of the Smaller Device is marked with the Apple trademark and the word "iPhone."

PROBABLE CAUSE

BACKGROUND ON AMTRAK

6. During the course of this investigation, your affiant learned details about how AMTRAK affects interstate commerce. Congress created the National Railroad Passenger Corporation, doing business as AMTRAK, as a private, for-profit Government corporation, pursuant to the passage of the Rail Passenger Service Act of 1970, to operate a nationwide system of passenger rail transportation.

7. AMTRAK receives significant federal funding through U.S. Department of Transportation (DOT) grants to cover its activities associated with the Northeast Corridor and the National Network as authorized by the Fixing America's Surface Transportation Act (*see* Div. A; Pub. L. No. 114-94).

8. In addition to providing a substantial portion of AMTRAK's funding, the federal government also provides oversight of how the funds are spent. The Federal

Railroad Administration (FRA), as part of the DOT, administers the grants to AMTRAK and provides federal oversight of AMTRAK's grants.

9. AMTRAK's ownership and corporate structure are heavily controlled by the federal government. The United States Government, through the Secretary of the United States Department of Transportation, owns all issued and outstanding preferred AMTRAK stock.

10. Pursuant to 49 U.S.C. § 24302, AMTRAK's ten-member Board of Directors is composed of the Secretary of the United States Department of Transportation; eight other board members appointed by the President of the United States and confirmed by the United States Senate; and the President of AMTRAK, who is appointed by the members of the Board. In selecting individuals for nomination to the Board, the President shall consult with the Speaker of the House of Representatives, the minority leader of the House of Representatives, the majority leader of the Senate, and the minority leader of the Senate to try to provide adequate and balanced representation of the major geographic regions of the United States served by AMTRAK. These branches of the federal government exercise substantial supervision over AMTRAK's operations. AMTRAK is required to submit annual reports to Congress and the President of the United States detailing such information as route-specific ridership and on-time performance. Congress conducts oversight hearings to delve into details of AMTRAK's budget, routes, and prices. In addition, the Freedom of Information Act (5 U.S.C. § 552) applies to AMTRAK.

11. AMTRAK has been substantially supported by federal funds. In recent years, AMTRAK has received over $1 billion in federal appropriations each year. AMTRAK is an "agency" of the federal government within the meaning established in Title 18, United States Code, Section 6, which defines "agency" as "any department, independent establishment, commission, administration, authority, board or bureau of the United States or any corporation in which the United States has a proprietary interest, unless the context shows that such term was intended to be used in a more limited sense."

INCIDENT AND INVESTIGATION

12. The Bureau of Alcohol, Tobacco, Firearms and Explosives, the Philadelphia Fire Marshal's Office, and AMTRAK Police are investigating a fire at the William H. Gray III 30th Street Station located at 2955 Market Street, Philadelphia, Pennsylvania, commonly referred to as 30th Street Station. 30th Street Station is a railroad station owned by AMTRAK, which is engaged in interstate commerce by providing commercial passenger rail service to destinations outside the Commonwealth of Pennsylvania. The fire resulted in property damage including damage to the building.

13. On March 7, 2023, at approximately 4:37 a.m., the Philadelphia Fire Department (PFD) was dispatched to 30th Street Station for an activated fire alarm. Additional communications were received from AMTRAK police that reported a fire in an electrical switch room. The fire department response was upgraded which caused additional units of fire apparatus to be dispatched.

14. 30th Street Station is a large, multi-level, concrete train station located at the corner of Market Street and 30th Street in Philadelphia, Pennsylvania. The building was occupied by patrons and AMTRAK employees at the time of the fire. There were no injuries or deaths reported because of the fire.

15. The fire occurred in an electrical switch room that was designated as "Garage Sub North" located on the parking garage level of 30th Street Station. The electrical switch room consists of two, interconnected rooms, each housing electrical switch gear (Garage Sub North and Garage Sub South). The PFD suppressed the fire, which involved a pallet of equipment in cardboard boxes stored in Garage Sub North. The fire resulted in property damage to the contents of the pallet as well as heat and smoke damage to Garage Sub North.

16. The Philadelphia Fire Marshal's Office (FMO) was dispatched to the scene to determine the origin and cause of the fire. FMO Lieutenant Kevin Collins requested the assistance of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) Arson and Explosives Task Force, which included your affiant.

17. Investigators examined the fire scene which included the remains of a pallet of 20/175-watt ballast kits contained in cardboard boxes as well as a pallet jack that was immediately adjacent.[1] The examination also documented heat and smoke damage to

[1] A ballast is an electrical device used with certain types of light fixtures. The ballast is a collection of electronic components used to produce the voltages and currents necessary to start the lamp and regulate its operation.

the walls and floor of Garage Sub North as well as damage to a ground bus that traversed horizontally along the walls approximately one foot above the floor.

18. Investigators examined potential accidental ignition sources for the cardboard boxes of ballast kits in Garage Sub North. The preliminary examination provided no viable accidental ignition scenarios for the cardboard boxes of ballast kits in Garage Sub North.

19. Your affiant consulted with an ATF Electrical Engineer regarding accidental ignition scenarios for the 20/175-watt ballast kits. The ATF Electrical Engineer provided a preliminary statement that there are no viable accidental ignition scenarios that would involve the ignition of the cardboard boxes by the 20/175-watt ballast kits.

20. Investigators recovered videos that showed a black male with a thin build, wearing a dark-colored, hooded, winter coat with a gray label/lettering on the left front, a fluorescent cap, a fluorescent shirt (underneath the winter coat), baggy, light-colored sweatpants, and dark shoes with light-colored soles (later identified as NASIR BILAAL). BILAAL wore a beard with black hair (See Figures 1 through 3).

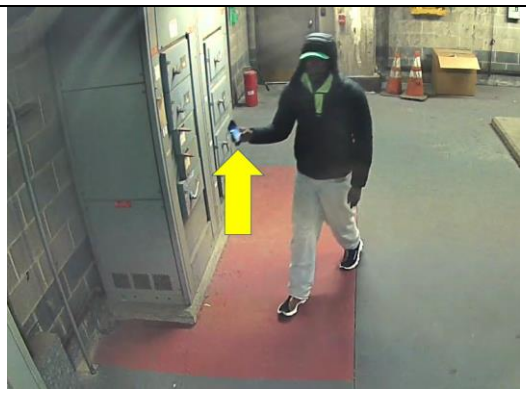

Figure 1 - BILAAL walking in Garage Sub South. Note the cellular telephone in his right hand with the screen illuminated (source: Amtrak).

Figure 2 - BILAAL walking in Garage Sub South. Note the cellular telephone in his right hand with the screen illuminated (source: Amtrak).

Figure 3 - Close up of BILAAL's smart phone. Note the illuminated screen (source: Amtrak).

21. In the video, BILAAL can be seen walking inside Garage Sub South. BILAAL is holding the cellular telephone up and in his right hand. The screen of the cellular telephone is illuminated. BILAAL appears to be either video recording the equipment in Garage Sub South or live streaming a video of the equipment in Garage Sub South to an unknown third party.

22. BILAAL walks through a doorway from Garage Sub South and into Garage Sub North at approximately 04:31:43 a.m., out of view of the camera. At approximately 04:32:31 a.m., approximately 48 seconds later, BILAAL can be seen running from Garage Sub North, through Garage Sub South, into the adjacent parking garage. BILAAL moves out of the view of the surveillance cameras and re-emerges with a dark-colored backpack. BILAAL then exits the building up a vehicular ramp at approximately 04:33:33 a.m. with the dark-colored backpack (See Figure 4).

Figure 4 - BILAAL exiting 30th Street Station via a vehicular ramp (source: Amtrak).

23. At approximately 04:34:45 a.m., approximately three minutes and two seconds after BILAAL entered Garage Sub North, and approximately two minutes, fourteen seconds after BILAAL was observed running from Garage Sub North, the emergency lights for the fire alarm activated.

24. Your affiant consulted with Amtrak Police who reviewed the surveillance video from the parking garage around Garage Sub North and Garage Sub South as well as surveillance video from inside Garage Sub South. AMTRAK Police reported the last persons to enter Garage Sub South prior to BILAAL did so on March 6, 2023, the day before the fire. AMTRAK employees also reported there was no fire within Garage Sub North when they were last present on March 6, 2023.

25. Investigators canvassed the area for surveillance video that would assist in the identification of BILAAL. Investigators tracked BILAAL's flight path out of the north side of the 30th Street Station parking garage and east on John F. Kennedy Boulevard past the PECO Energy building. Investigators also reviewed video of BILAAL taken from inside 30th Street Station prior to the fire.

26. The prior evening, Monday, March 6, 2023, at approximately 8:00 p.m., BILAAL was captured on surveillance video purchasing an AMTRAK train ticket. Further review of the video showed BILAAL provided identification and purchased the ticket in cash.

27. A review of the ticket purchase showed the purchaser identified himself as NASIR BILAAL. BILAAL used an expired Pennsylvania identification card as his identifying document to purchase the ticket. BILAAL was in possession of a dark-colored backpack. A lighter-colored stripe was visible along the length of the strap of the backpack.

28. A search of the Pennsylvania Justice Network for the name "NASIR BILAAL" produced a result for NASIR BILAAL who is a black male born on June 15, 2000. BILAAL is reported to be five feet, eight inches in height and has brown eyes. The photograph produced by the Pennsylvania Justice Network search shows BILAAL having a beard with black hair (See Figures 5 and 6). Your affiant compared these images to images of BILAAL (See Figures 7 through 10).

Figure 5 - Photograph of Nasir BILAAL taken in December 2022 (source JNET).

Figure 6 - Photograph of Nasir BILAAL taken in March 2021 (source PennDOT).

Figure 7 - Photograph of BILAAL walking within Garage Sub South (source Amtrak).

Figure 8 - Photograph of Nasir BILAAL purchasing a train ticket. Note the dark-colored backpack with a lighter-colored stripe on the strap indicated by the arrow (source Amtrak).

Figure 9 - Nasir BILAAL purchasing a train ticket (source Amtrak).

Figure 10 - Nasir BILAAL purchasing a train ticket. Note the dark-colored backpack indicated by the arrow (source Amtrak).

28. Based on the video evidence and the examination of the fire scene, investigators have preliminarily classified the cause of the fire as incendiary, meaning a

fire that is willfully ignited in an area or under circumstances where and when there should not be a fire (the pallet of materials inside Garage Sub North.).

29. On Friday, March 17, 2023, NASIR BILAAL was detained by the Lansdowne Police department in Lansdowne, Pennsylvania pursuant to a Federal Arrest warrant. The Lansdowne Police took custody of BILAAL's property which included two Apple iPhone cellular telephones. BILAAL's property was subsequently transferred to the custody of your affiant.

30. Your affiant transported BILAAL to the Federal Detention Center in Philadelphia, Pennsylvania.

31. The cellular telephones found in BILAAL's possession on March 17, 2023, are similar in size and color to the cellular telephone observed in BILAAL's possession during his time in Garage Sub South on March 7, 2023, as captured on video from the AMTRAK video surveillance system.

Figure 4 - Larger of the two iPhones found in BILAAL's possession on March 17, 2023, at the time of his arrest.

Figure 5 - Smaller of the two iPhones found in BILAAL's possession on March 17, 2023, at the time of his arrest.

32. Your affiant believes one of the two cellular telephones found in BILAAL's possession on March 17, 2023, is the same cellular telephone observed being used by him to either video record or live stream the equipment in Garage Sub South just prior to the fire in Garage Sub North.

33. Based on the above information, your affiant has probable cause to believe that evidence of the arson at 30th Street Station on March 7, 2023, to include a video

recording of the of equipment in Garage Sub South on March 7, 2023, as well as evidence of the initiation of the fire can, be found stored on one of the two cellular telephones found on BILAAL's person at the time of his arrest on March 17, 2023.

TECHNICAL TERMS

34. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. "Digital device," as used herein, includes the following three terms and their respective definitions:

1. A "computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

2. "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage

media include, but are not limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

3. "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. "Wireless telephone" (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through "wi-fi" networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional "land line" telephones, computers, and other digital devices. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities.

These include, variously: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system ("GPS") locating and tracking technology, and accessing and downloading information from the Internet.

c. A "tablet" is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, "wi-fi" networks, or otherwise. Tablets typically contain programs called applications ("apps"), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

d. A "GPS" navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated "GPS") to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical

representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. Internet Protocol ("IP") Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series

of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. The "Internet" is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. "Internet Service Providers," or "ISPs," are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line ("DSL"), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the

subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

j. A "modem" translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

k. A "router" often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

l. "Domain Name" means the common, easy-to-remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically ".com" for commercial organizations, ".gov" for the governmental organizations, ".org" for organizations, and ".edu" for educational organizations. Second-level names will further identify the organization, for example "usdoj.gov" further identifies the United States governmental agency to be the Department of Justice.

Additional levels may exist as needed until each machine is uniquely identifiable. For example, "www.usdoj.gov" identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

m. "Cache" means the text, image, and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

n. "Peer to Peer file sharing" (P2P) is a method of communication available to Internet users through the use of special software, which may be downloaded from the Internet. In general, P2P software allows a user to share files on a computer with other computer users running compatible P2P software. A user may obtain files by opening the P2P software on the user's computer and searching for files that are currently being shared on the network. A P2P file transfer is assisted by reference to the IP addresses of computers on the network: an IP address identifies the location of each P2P computer and makes it possible for data to be transferred between computers. One aspect of P2P file sharing is that multiple files may be downloaded at the same time. Another aspect of P2P file sharing is that, when downloading a file, portions of that file may come from multiple other users on the network to facilitate faster downloading.

i. When a user wishes to share a file, the user adds the file to shared library files (either by downloading a file from another user or by copying any file into the shared directory), and the file's hash value is recorded by the P2P software. The hash value is independent of

the file name; that is, any change in the name of the file will not change the hash value.

ii. Third party software is available to identify the IP address of a P2P computer that is sending a file. Such software monitors and logs Internet and local network traffic.

o. "VPN" means a virtual private network. A VPN extends a private network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if they were an integral part of a private network with all the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from a private network-hence the name "virtual private network." The communication between two VPN endpoints is encrypted and usually cannot be intercepted by law enforcement.

p. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded.

Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

q. "Malware," short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

35. Based on my training, experience, and research, I know that the Devices, Apple I-phones, have capabilities that allow it to serve as a wireless telephone, a digital camera, a portable media player, a GPS navigation device, and to access the internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, and sometimes by implication who did not, as well as location information and evidence relating to the commission of the offense under investigation.

COMPUTERS, ELECTRONIC/MAGNETIC STORAGE AND FORENSIC ANALYSIS

36. As described above and in Attachment B, this application seeks permission to search for evidence that might be found within the Devices, in whatever form they are found. Based on my knowledge, training, and experience, as well as

information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that there is probable cause to believe that the records and information described in Attachment B will be stored in the Devices for at least the following reasons:

a. Individuals who engage in criminal activity, including Title 18, United States Code, Section 844 (i) (maliciously damaging or destroying, or attempting to damage or destroy, by means of fire any building used in interstate commerce) use digital devices, like the Device(s), to access websites to gain knowledge and facilitate illegal activity; keep a record of purchases made in furtherance of the arson; create audio and/or video recordings of the arson; and communicate on the Devices via voice calls and text messages before, during, and after the arson. Also, as noted above, the recovered surveillance video of the incident reveals that BILAAL was utilizing his phone immediately prior the fire likely by either recording a video or making a live-stream. I therefore submit that probable cause exists to believe that evidence of the incident will be recovered from the Devices.

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often "back up" or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

37. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Device(s) at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a

word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

38. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery of "residue" of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement

laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting "keyword"

search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart

phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information,

records, or evidence within the scope of this warrant. In searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

g. The digital devices, and/or any digital images thereof created by law enforcement, sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

h. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by "opening," reviewing, or reading the images or first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "keyword" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In

addition, the forensic examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the Device(s) will be specifically chosen to identify the specific items to be seized under this warrant.

AUTHORIZATION TO SEARCH AT ANY TIME OF THE DAY OR NIGHT

39. Because forensic examiners will be conducting their search of the digital devices in a law enforcement setting over a potentially prolonged period of time, I respectfully submit that good cause has been shown, and therefore request authority, to conduct the search at any time of the day or night.

CONCLUSION

I submit that this affidavit supports probable cause for a warrant to search the devices described in Attachment A and to seize the items described in Attachment B.

Respectfully submitted,

/s Chad D. Campanell
CHAD D. CAMPANELL
Senior Special Agent – CFI
Bureau of Alcohol, Tobacco, Firearms & Explosives

Sworn and Subscribed to before me

this 4th day of April, 2023

s/ Scott W. Reid
HONORABLE SCOTT W. REID
United States Magistrate Judge
Eastern District of Pennsylvania

ATTACHMENT A

Property to be searched

The property to be searched are two Apple iPhone cellular telephones recovered from the person of NASIR BILAAL. The cellular telephones are locked, and the serial numbers and other identifying information are unknown. The cellular telephones are physically located at the ATF Group II Office located at 200 Chestnut Street, Room 504, Philadelphia, Pennsylvania, 19106.

The first phone is the larger of the two cellular telephones ("Larger Device"). The model number is unknown. The Larger Device is approximately six inches in height and three inches in width. The Larger Device has damage in the form of broken glass on the rear of the phone in the lower left corner as well as damage on the rear of the phone in the upper right corner. The Larger Device has one camera lens on the back side as well as a single flashlight. The rear of the Larger Device is marked with the Apple trademark and the word "iPhone."

The second phone is the smaller of the two cellular telephones ("Smaller Device"). The model number is unknown. The Smaller Device is approximately five and a half inches in height and two and five-eighths inches in width. The Smaller Device has no visible physical damage. The Smaller Device has one camera lens on the back side as well as a single flashlight. The rear of the Smaller Device is marked with the Apple trademark and the word "iPhone."

ATTACHMENT B

Property to be seized

The items, information, and data to be seized are evidence relating to, in whatever form and however stored, violations of Title 18, United States Code, Section 844 (i) (maliciously damaging or destroying, or attempting to damage or destroy, by means of fire any building used in interstate commerce), as described in the search warrant affidavit, including, but not limited to:

a. Records and information relating to the identity or location of perpetrators, aiders and abettors, coconspirators, and accessories after the fact;

b. Records and information relating to communications with Internet Protocol addresses;

c. Records and information that constitute evidence of the state of mind of NASIR BILAAL, *e.g.*, intent, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation.

d. Records and information that constitute evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts.

e. Evidence of who used, owned, or controlled the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;

f. Evidence of software, or the lack thereof, that would allow others to control the Device(s), such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

g. Evidence of the attachment to the Device of other storage devices or similar containers for electronic evidence;

h. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device;

i. Evidence of the times the Device was used;

j. Passwords, encryption keys, and other access devices that may be necessary to access the Device;

k. Documentation and manuals that may be necessary to access the Device(s) or to conduct a forensic examination of the Device(s);

l. Records of or information about Internet Protocol addresses used by the Device(s); and

m. Records of or information about the Device(s)'s Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.